

Amendment Dated December 27, 2007
Serial No. 10/666,529

REMARKS

Reconsideration of the rejections set forth in the Office Action is respectfully requested. By this Amendment claims 1 and 10-12 have been amended. Currently, claims 1-17 are pending in this application.

Rejection under 35 USC 101

Claims 10-12 were rejected under 35 USC 101 as non-statutory. Specifically, the Examiner has taken the position that the claims are non-statutory as functional descriptive material. Applicants have amended the claims to overcome this rejection and respectfully request that it be withdrawn.

Rejection under 35 USC 103

Claims 1-5, 7, 9-15, and 17 were rejected under 35 USC 103 as unpatentable over Samarasinghe (U.S. Patent Application Publication No. 2004/0028080) in view of Takeda (U.S. Patent Application Publication No. 2003/0110292) and Hama (U.S. Patent No. 7,707,346). Additionally, claims 6 and 8 were rejected over Samarasinghe, Takeda, and Hama, and further in view of Donovan (U.S. Patent Application Publication No. 2002/0041590). These rejections are respectfully traversed in view of the amendments to the claims and the following arguments.

This application relates to the provision of Virtual Private Network (VPN) services on demand. For example, as explained at page 4, line 26 to page 5, line 5, this application describes a two step process for allowing VPN resources to be obtained on demand. First, VPN tunnels (label switched paths) are established through an MPLS network. Then, resources on the network VPN tunnels are reserved to handle traffic between participants in an enterprise VPN so that traffic may be passed between the participants.

In one embodiment, applicants propose to integrate SIP signaling with network VPN UNI/NNI signaling to enable enterprise VPN applications to use familiar SIP signaling to reserve network VPN resources without understanding the nature or details associated with the network VPN resources. A gateway on the network intercepts the SIP signaling and performs the UNI/NNI signaling to reserve resources on the VPN tunnels (label switched paths) through the network so VPN resources may be obtained on behalf of the applications. (See Specification at page 4, lines 15-23).

Amendment Dated December 27, 2007
Serial No. 10/666,529

The Examiner has cited a combination of three references, which the Examiner contends would have made this process obvious. If applicants are understanding the Examiner's rejection correctly, the Examiner has taken the position that:

- Samarasinghe teaches SIP signaling but doesn't mention VPNs.
- Takeda teaches that SIP signaling may include various parameters, but doesn't mention VPNs.
- Hama teaches VPNs, but doesn't mention SIP.

The Examiner then concludes that it would have been obvious to have VPNs in Samarasinghe's network in order to provide a secured partition of a network. Additionally, the Examiner concludes that it would have been obvious to include VPN information in SIP messages and register VPN information in Samarasinghe in order to provide call setup within a VPN network or to update the topology of the VPN network.

Applicants respectfully submit that it would not have been obvious to use SIP signaling to reserve network VPN resources. Specifically, although network VPNs were known at the time of the invention, they were conventionally statically provisioned and set up by the network provider before-hand. Thus, the notion of on-demand network VPNs was not something that was known in the industry and not something that would have been obvious to implement.

Additionally, although SIP signaling was a known way of establishing sessions between users, it was intentionally intended to not be used to reserve resources on the underlying network.

In an Information Disclosure Statement dated December 15, 2003, applicants submitted a copy of IETF RFC 3261 which defines SIP. Note, that RFC 3261 obsoletes RFC 2543 referred to by Takeda (Takeda at Par. 4). Although the standard is quite lengthy, the overview (Section 2, pages 8-9) is instructive as to how SIP operates. As stated in this section "Since SIP messages and the sessions they establish can pass through entirely different networks, SIP cannot, and does not, provide any kind of network resource reservation capabilities." Thus, SIP was explicitly designed to not be used to reserve resources on the underlying network. Applicants have used SIP contrary to this statement to allow network VPN services to be created and reserved on demand.

A person of ordinary skill in the art would understand how SIP signaling was intended to operate, and know that SIP signaling was used to establish sessions on the network and not as a

Amendment Dated December 27, 2007
Serial No. 10/666,529

resource reservation tool. Nothing in the several references cited by the Examiner suggests that SIP should be used in a contrary manner. Thus, applicants respectfully submit that a person of ordinary skill in the art would not have been motivated to combine the references as suggested by the Examiner.

Going back to the rejection, the Examiner has taken the position that Samarasinghe and Takeda teach the use of SIP signaling but do not mention that it should be used to signal VPNs. Hama teaches normal MPLS signaling but doesn't mention SIP signaling.

Previously, before the Supreme Court's decision in KSR International Co. v Teleflex, Inc., 82 USPQ2d 1385 (2007) it was necessary to find some teaching, suggestion, or motivation to make a combination to find claims to the combination obvious. The Supreme Court overruled the rigid teaching, suggestion, motivation test, and instead stated that when considering obviousness, the operative question is whether the improvement is more than the predictable use of prior art elements according to their established functions. (See Federal Register, Vol. 42, No. 195, at pages 57527-35, October 10, 2007).

In this case, applicants have used pieces of networking that were designed for different purposes and put them together in a novel way to achieve something that was not achievable before, and which would not have been obvious to a person of ordinary skill in the art. Moreover, applicants are using one of the pieces, SIP signaling, in a manner contrary to its stated purpose. Thus, applicants have not merely taken known prior art elements and used them according to their established functions, but rather have taken elements and used them in unintended ways to allow VPNs to be obtained on demand.

Specifically, as noted by applicant at page 2 lines 4-20, at the time of the invention there were two general VPN solutions -- network based VPNs and Enterprise VPNs. Network VPNs were commonly implemented according to IETF RFC 2547, as discussed in great detail by Hama. Enterprise VPNs, by contrast, were focused at the application level to allow distributed workflow logic and resource management, coordinated failover between participants, problem determination, QoS, and security semantics. These Enterprise VPNs were thus focused on the application level to allow applications on different machines to work together. Enterprise VPNs thus didn't focus on the network, but instead relied on network VPNs to carry traffic between the participants.

Amendment Dated December 27, 2007
Serial No. 10/666,529

Applicants then determined that it would be desirable to have an interface between network VPNS and the enterprise VPNs to enable network VPN services to be provided on demand. (see Specification at page 2, lines 24-26).

At the time of the invention, network VPNs were statically set up. For example, Hama teaches that MPLS tunnels are established using an outer label, and that VPNs are implemented using an inner label. This is commonly referred to as label stacking. First, the provider would establish a label switched path (LSP) through the network. The outer label would be used to put traffic onto the LSP and switched by intermediate routers as the traffic crossed the MPLS network. A second label (inner label) would also be applied to the packet and used to differentiate traffic on different VPNs. The ingress router would apply the inner label to tag a packet as belonging to a VPN, and the egress router would read the inner label to determine which VPN the packet belonged to. All the labels would be set up "beforehand" and not on demand. (Hama at Col. 5, lines 20-21). Thus, as taught by Hama, a VPN service provider would establish the LSP (outer label) and establish VPNs within the LSP (inner label) beforehand. The VPNs could then be used by customers.

Samarasinghe and Takeda both teach the use of SIP signaling in the normal manner. In Samarasinghe, a SIP Invite is sent to a call control element, where it is redirected to various other components on the network. For example, the call control element may forward the SIP invite to a network routing engine 33, a media server 30, a service broker 36, or one of the other elements on the network. (See Samarasinghe at Fig. 2). Once the signaling portion has completed to set up the session, the session is implemented on a media path that is independent of the signaling path. As noted by Samarasinghe, the media path generally does not involve the call control element 24 that is in charge of the signaling (Samarasinghe at Par. 21). Thus, Samarasinghe uses SIP in the normal manner of isolating the signaling from the media path. Nothing in Samarasinghe suggests that SIP signaling is being used to reserve resources on the network.

Takeda also uses SIP in a normal manner. Takeda teaches that the SIP invite message should include a message header having a message header and a message body. The message header has a VIA field that identifies a route of the SIP message and allows the responder to send a response back over the same route. The message also includes a To header indicating the destination of the SIP message and a From header that indicates the initiator of the message. A call-ID header is used to indicate a call identifier. The message also includes a c-parameter that

Amendment Dated December 27, 2007
Serial No. 10/666,529

indicates connection information, an m-parameter that indicates a port through which data is received. After establishing the session, audio information between the terminals is sent to the destination (connection/port) identified by the c and m parameters. (Takeda at Par. 158). Thus, Fig. 8 of Takeda shows the generic format for a SIP invite, which contains parameters relevant to the signaling path and the c and m parameters which state the connection/port over which the media will be transmitted. The SIP invite of Fig. 8 does not contain parameters relevant to reserving resources on the network

Accordingly, nothing in Samarasinghe or Takeda teaches or suggests that SIP should be used to reserve resources on the network. In view of the statement in the underlying SIP protocol that "SIP cannot, and does not, provide any kind of network resource reservation capabilities." applicants respectfully submit that it would not have been obvious to combine the references as suggested by the Examiner.

The preceding arguments set the background as to why the cited combination of references would not have made it obvious to implement the solution adopted by applicants. Of course, the measure of whether a claim is patentable hinges entirely on what is recited in the claim.

Claim 1 recites a method including the steps of receiving a Session Initiation Protocol (SIP) message containing VPN information from an initiating application, and registering the VPN information from the SIP message on a communication network. This claim contains two aspects that would not have been obvious in view of the cited combination of references. First, the claim recites that the SIP message contains VPN information from an initiating application. The combination of references would not have taught or suggested that the SIP message should contain VPN information. Additionally, independent claim 1 recites that the VPN information from the SIP message is registered on a communication network. This step involves registering the VPN information on the network, rather than signaling establishment of a session. As noted above, SIP teaches away from using SIP to reserve resources on the underlying network. Registering the VPN information is a first step in reserving VPN resources. (Specification at Page 5 line 12 to page 6, line 21). The combination of references does not provide any motivation for their combination, and the underlying standard discussed by the references explicitly teaches away from making the combination. In this instance, applicants respectfully

Amendment Dated December 27, 2007
Serial No. 10/666,529

submit that claim 1 is patentable over the cited combination and respectfully requests that the rejection be withdrawn.

Independent claim 10 recites a method including the steps of registering application-VPN-ID information associated with a first application on a communication network, and interfacing with the communication network to obtain network VPN resources associated with the application-VPN-ID information upon receipt of a request for access to the network VPN resources from the first application. This method requires two steps – an initial registration step and a later request for access to the network VPN resources. The Examiner does not appear to have addressed this two step process, and does not appear to have specifically addressed independent claim 10. Applicants respectfully submit that the combination of references does not show this new signaling method and thus respectfully request that the rejection of claim 10 be withdrawn.

Conclusion

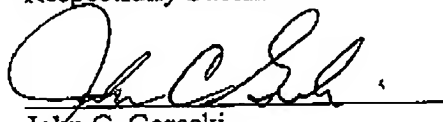
In view of foregoing claim amendments and remarks, it is respectfully submitted that the application is now in condition for allowance and an action to this effect is respectfully requested. If there are any questions or concerns regarding the amendments or these remarks, the Examiner is requested to telephone the undersigned at the telephone number listed below.

If any fees are due in connection with this filing, the Commissioner is hereby authorized to charge payment of the fees associated with this communication or credit any overpayment to Deposit Account No. 502246 (Ref: NN-16019).

Dated: December 27, 2007

John C. Gorecki, Esq.
P.O. Box 553
Carlisle, MA 01741
Tel: (978) 371-3218
Fax: (978) 371-3219
john@gorecki.us

Respectfully Submitted


John C. Gorecki
Registration No. 38,471